Hazard Analysis and Fault Tree Analysis

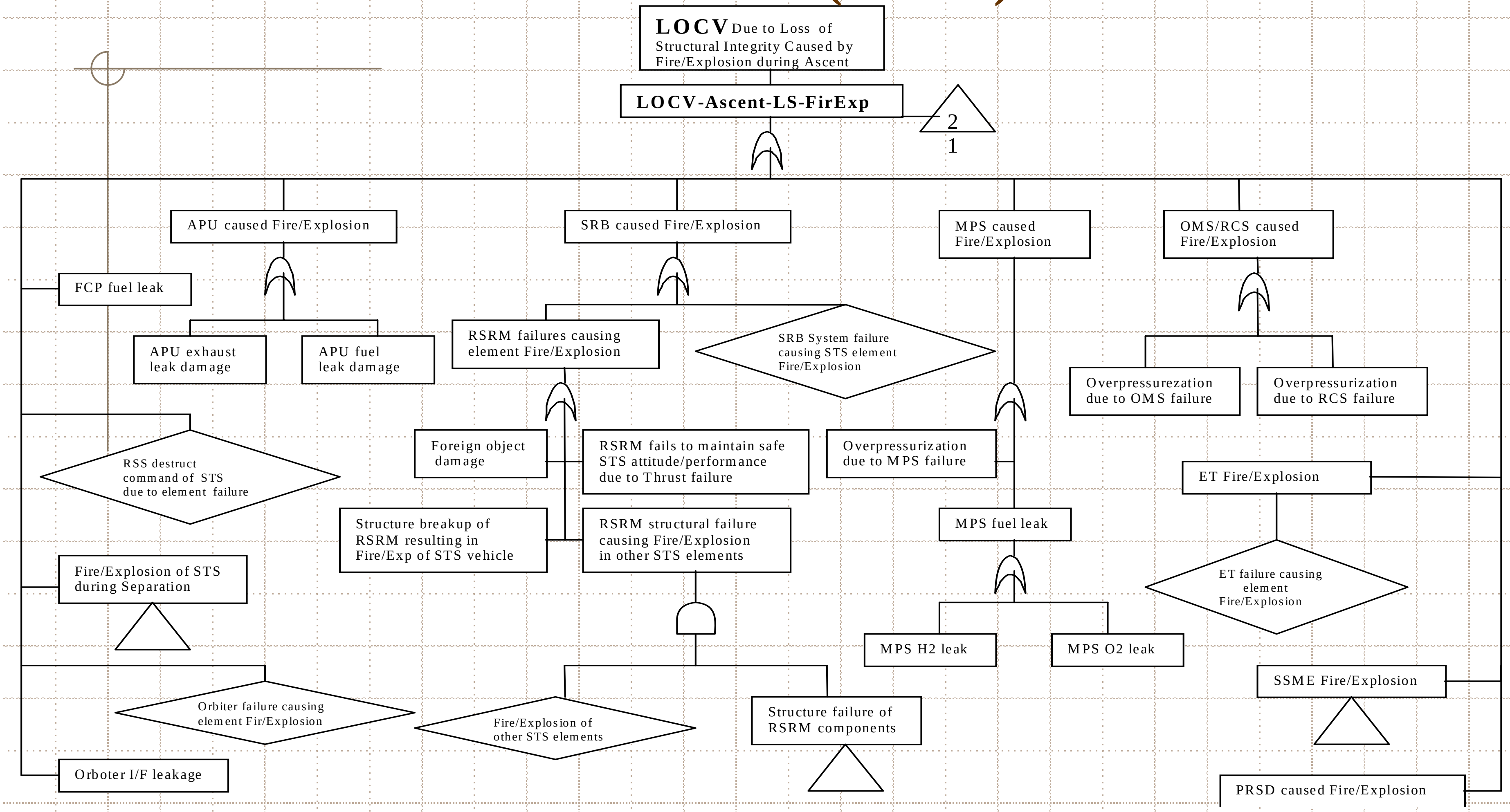
Bill Vesely

NASA HQ

Use of a Fault Tree in Identifying Hazards

- When a fault tree is used to identify the hazards then it is often called a Master Logic Diagram (MLD)
- The top event is the undesired event that can result from the hazards
- The top event is resolved to initiating events that can result in the undesired event
- Each initiating event is developed into an accident scenario to assess the associated risk
- Each initiating event is also linked to the conditions enabling the initiating event

A Master Logic Diagram for the Space Shuttle for Loss of Crew and Vehicle (LOCV) Due to Fire



LOCV Due to Loss of Structural Integrity Caused by Fire/Explosion during Ascent

LOCV-Ascent-LS-FirExp

2

1

APU caused Fire/Explosion

SRB caused Fire/Explosion

MPS caused Fire/Explosion

OMS/RCS caused Fire/Explosion

FCP fuel leak

APU exhaust leak damage

APU fuel leak damage

RSRM failures causing element Fire/Explosion

SRB System failure causing STS element Fire/Explosion

Overpressurezation due to OMS failure

Overpressurization due to RCS failure

RSS destruct command of STS due to element failure

Foreign object damage

RSRM fails to maintain safe STS attitude/performance due to Thrust failure

Overpressurization due to MPS failure

ET Fire/Explosion

Structure breakup of RSRM resulting in Fire/Exp of STS vehicle

RSRM structural failure causing Fire/Explosion in other STS elements

MPS fuel leak

Fire/Explosion of STS during Separation

ET failure causing element Fire/Explosion

MPS H2 leak

MPS O2 leak

SSME Fire/Explosion

Orbiter failure causing element Fir/Explosion

Fire/Explosion of other STS elements

Structure failure of RSRM components

Orboter I/F leakage

PRSD caused Fire/Explosion

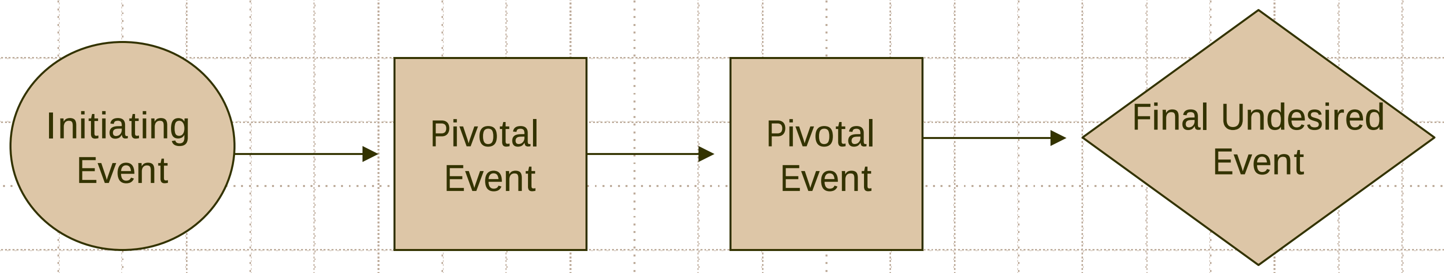
Constructing an Accident Scenario for Each Initiating Event

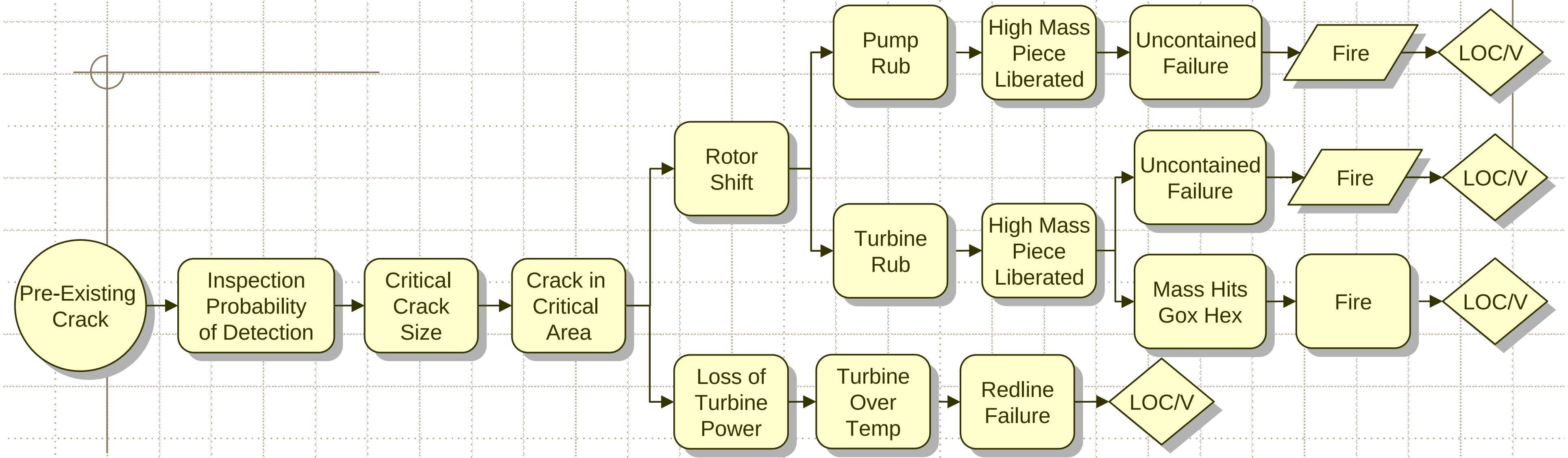
- The accident scenario defines additional enabling events (pivotal events) which are necessary for the initiating event to progress to the undesired final event
- The pivotal events in the accident scenario are resolved to basic causal events at which controls are applied
- The initiating event can also be resolved to more basic causal events where controls can be instituted

Approaches for Constructing the Accident Scenario

- Event Sequence Diagrams (ESDs) construct the accident scenario as a chain sequence
- Event Trees (ETs) construct the accident scenario as an event tree
- Fault Trees (FTs) construct the accident scenario as a fault tree

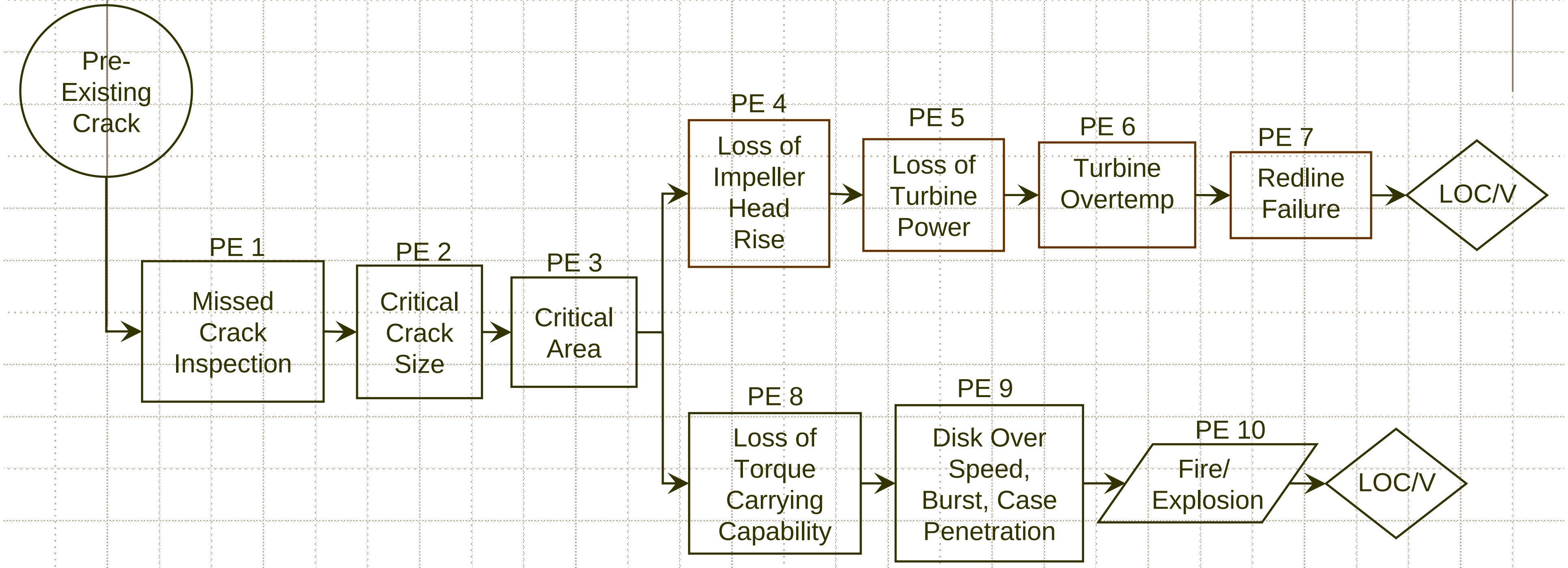
Illustration of a Basic Event Sequence Diagram



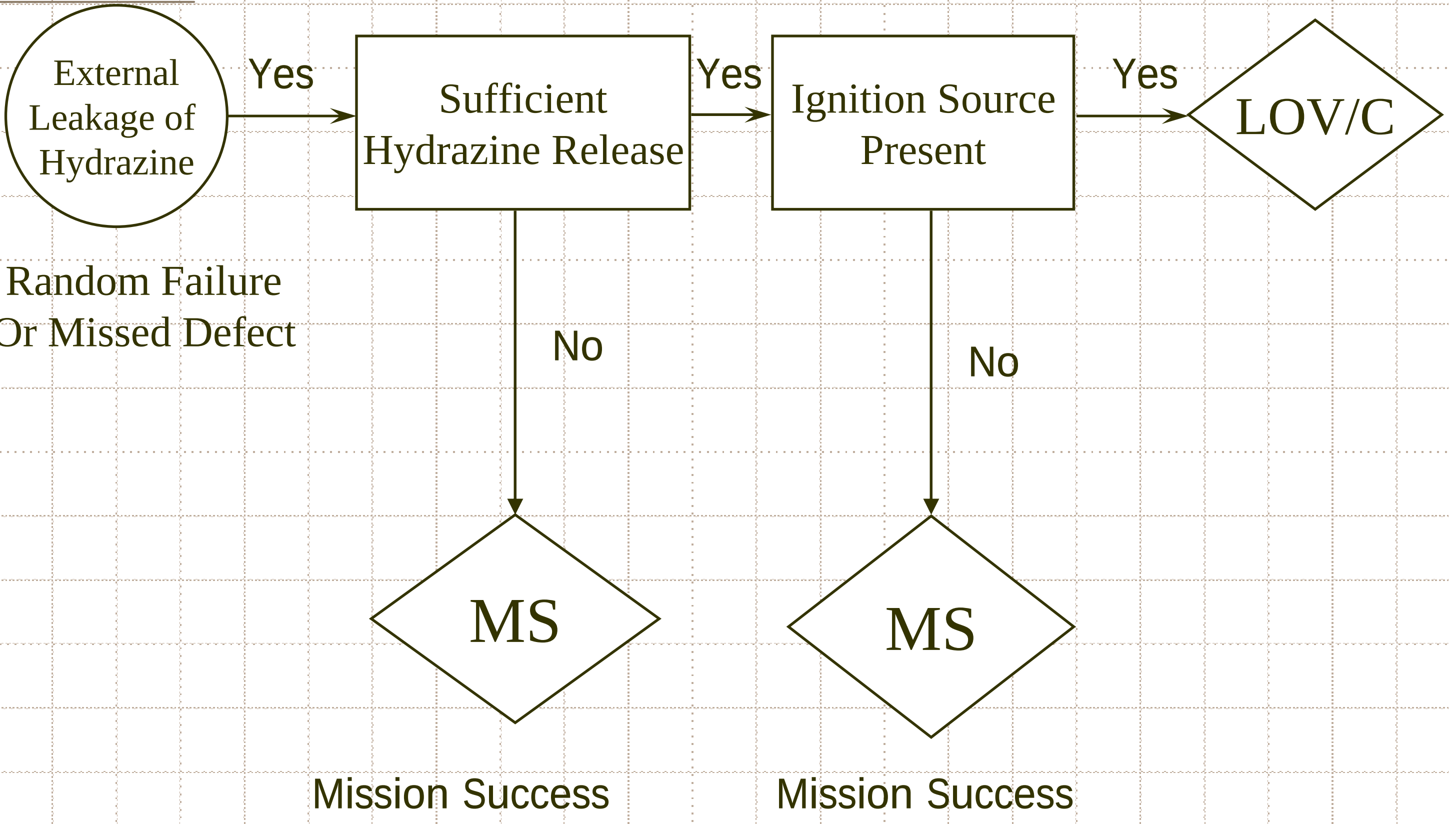


An Event Sequence Diagram (ESD) for a Hazard Analysis of Cracks Existing in the Turn-Around-Duct of the High Pressure Pump of the SSME

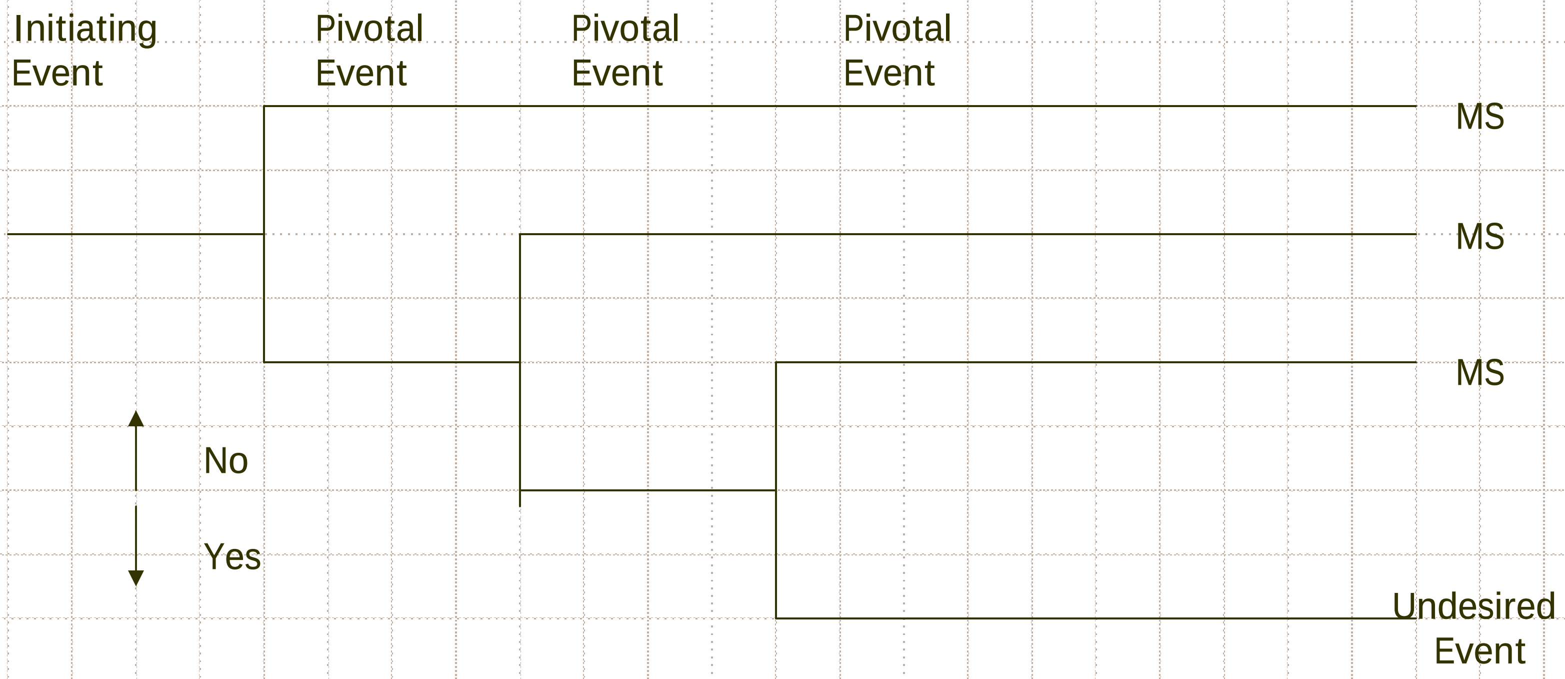
2nd Stage Impeller Blade ESD ~ Pre-Existing Flaw



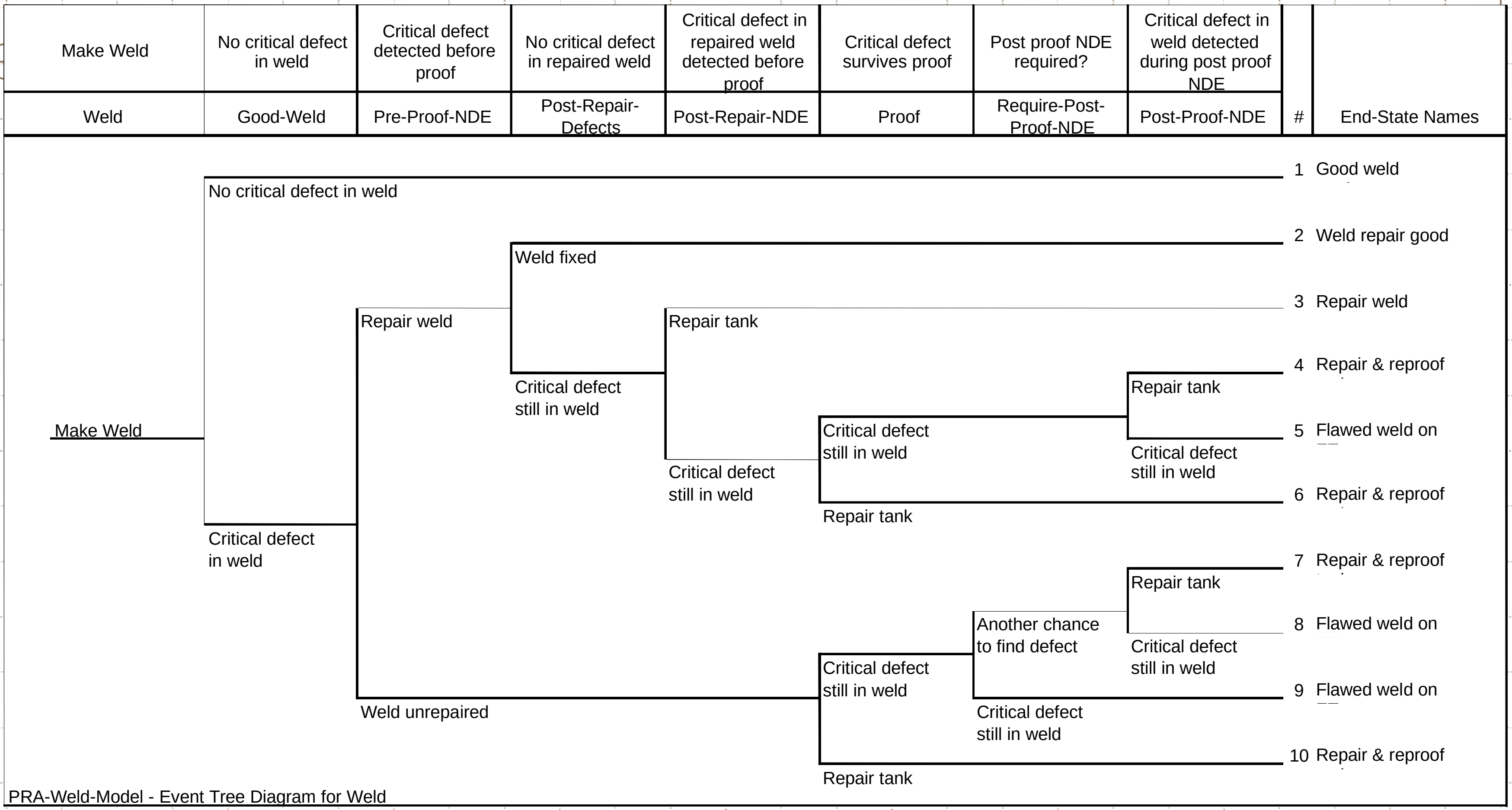
Event Sequence Diagram for External Leakage of Hydrazine in the APU


External Leakage of Hydrazine
Yes
Sufficient Hydrazine Release
Yes
Ignition Source Present
Yes
LOV/C
Random Failure Or Missed Defect
No
No
MS
MS
Mission Success
Mission Success

Basic Event Tree Model



ET Weld Defect Event Tree



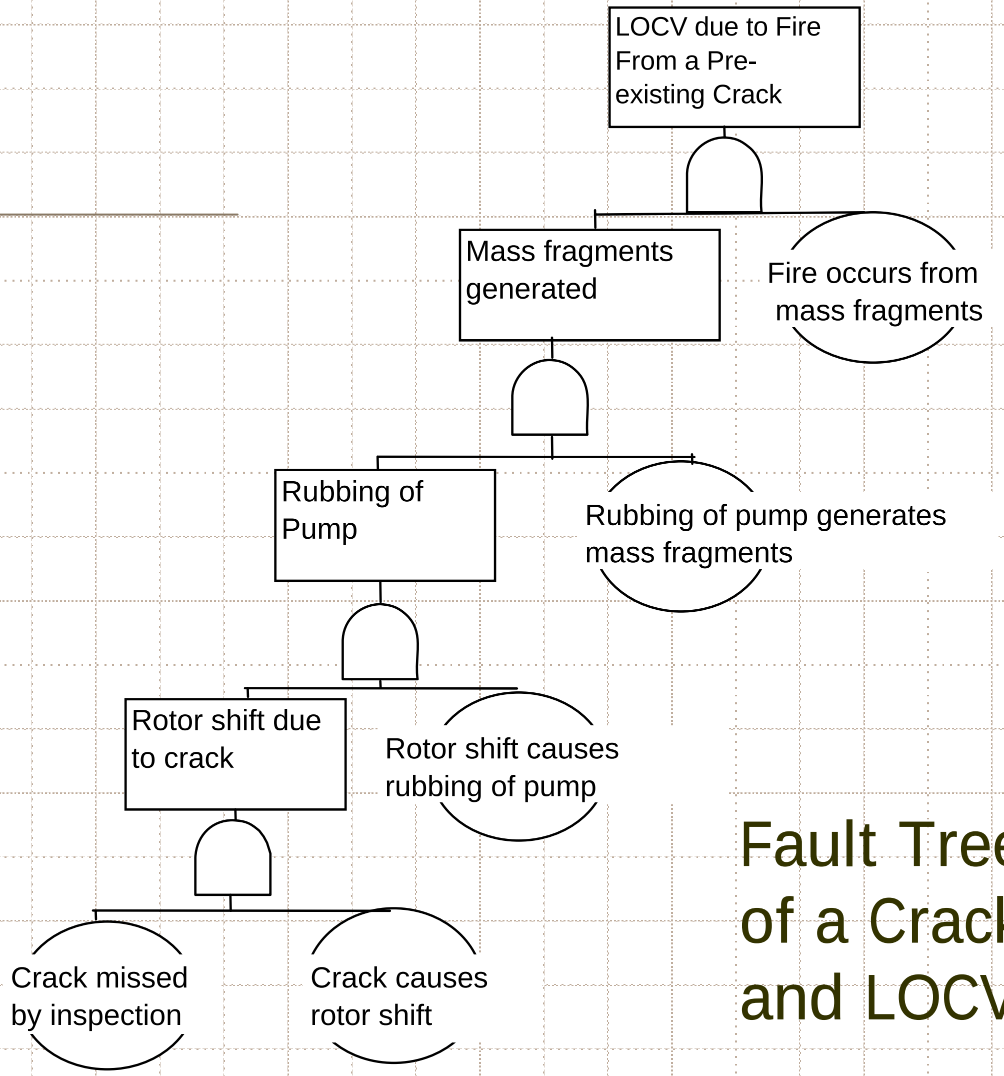
Make Weld	No critical defect in weld	Critical defect detected before proof	No critical defect in repaired weld	Critical defect in repaired weld detected before proof	Critical defect survives proof	Post proof NDE required?	Critical defect in weld detected during post proof NDE		
Weld	Good-Weld	Pre-Proof-NDE	Post-Repair-Defects	Post-Repair-NDE	Proof	Require-Post-Proof-NDE	Post-Proof-NDE	#	End-State Names

#	End-State Names
1	Good weld
2	Weld repair good
3	Repair weld
4	Repair & reproof
5	Flawed weld on
6	Repair & reproof
7	Repair & reproof
8	Flawed weld on
9	Flawed weld on
10	Repair & reproof

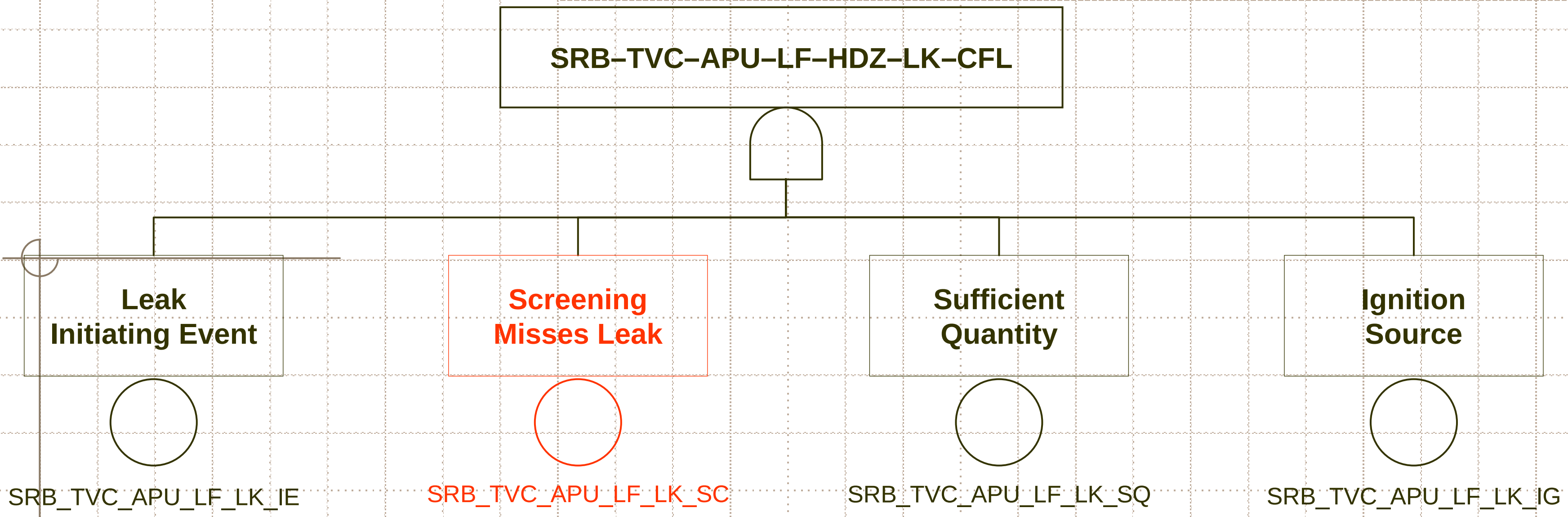
Make Weld
No critical defect in weld
Critical defect in weld
Repair weld
Weld unrepaired
Weld fixed
Critical defect still in weld
Repair tank
Critical defect still in weld
Critical defect still in weld
Repair tank
Repair tank
Critical defect still in weld
Critical defect still in weld
Repair tank
Another chance to find defect
Critical defect still in weld
Repair tank
Critical defect still in weld

PRA-Weld-Model - Event Tree Diagram for Weld

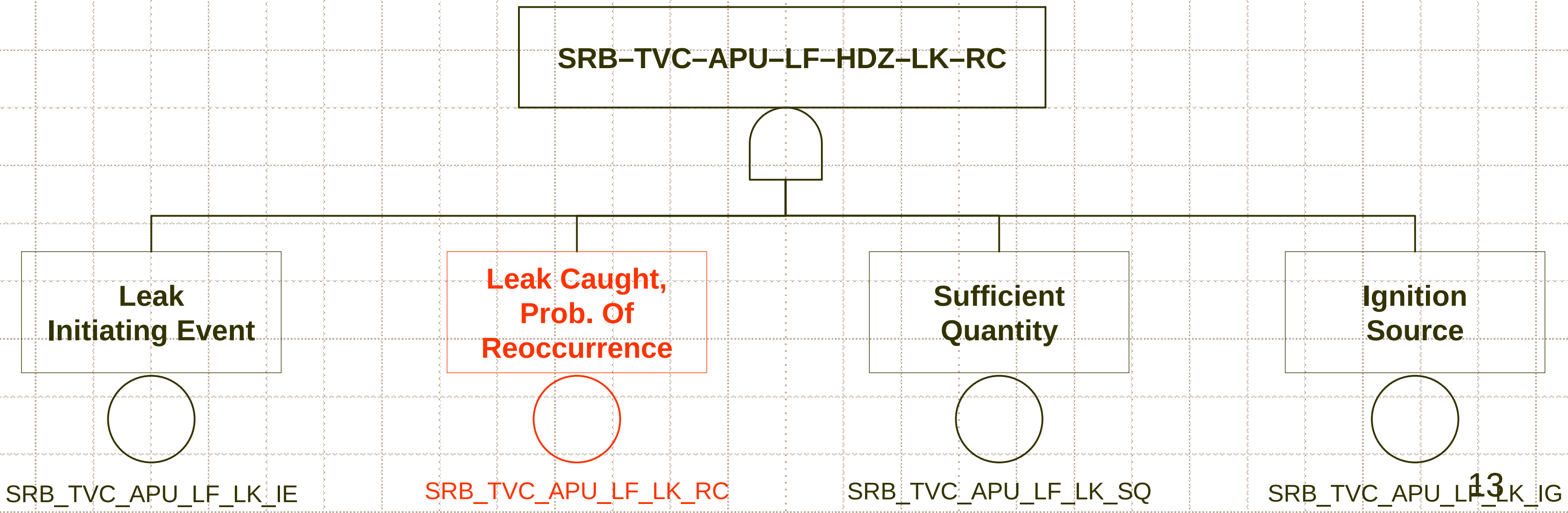
Weld Process Example


LOCV due to Fire From a Pre-existing Crack
Mass fragments generated
Fire occurs from mass fragments
Rubbing of Pump
Rubbing of pump generates mass fragments
Rotor shift due to crack
Rotor shift causes rubbing of pump
Crack missed by inspection
Crack causes rotor shift

Fault Tree for the Hazard of a Crack Causing a Fire and LOCV



Accident Scenarios Modeled in Fault Trees



A Fault Tree is Generally Not Recommended for Scenario Modeling

- An accident scenario generally involves a time sequence of events
- Accident scenario modeling is inductive and determines subsequent events and resulting consequences
- Accident scenarios are best modeled using ESDs or ETs
- A fault tree is a deductive model resolving an undesired event into primary causes
- FTs are best applied in resolving the events in an accident scenario to primary causal events

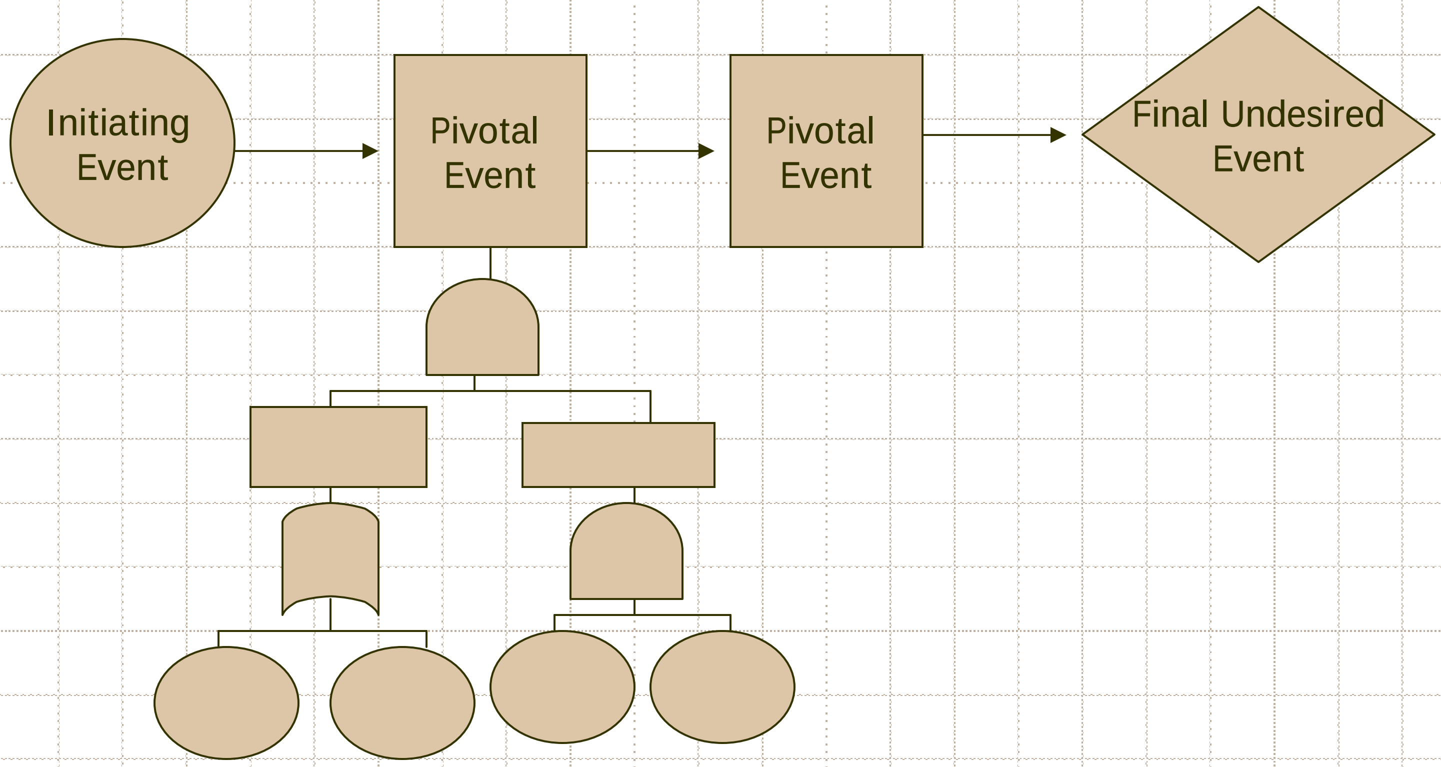
FTA Application in Resolving an Event to Basic Causal Events

- The top event of the FT is the initiating event or one of the enabling events in the accident scenario
- The FT is developed to basic causal events at which controls are applied
- The basic causal event description includes the relevant failure mode as done in standard FTA
- Primitive root causes of the basic causal event are not resolved unless controls are applied at this level

Use of a FT in Modeling System Failures in an Accident Scenario

- Certain of the enabling events (pivotal events) in the accident scenarios can in particular involve system failures
- A fault tree is then constructed for each system failure to resolve to component failures or basic causes
- The fault trees are then linked to the accident scenarios to evaluate the accident risks

Illustration of a Basic Event Sequence Diagram with a Linked Fault Tree



Reference

- **“Fault Tree Handbook with Aerospace Applications’, Version 1.1, NASA Publication, August 2002.**